

*Матеріали IV Міжнародної науково-технічної конференції молодих учених та студентів.
Актуальні задачі сучасних технологій – Тернопіль 25-26 листопада 2015.*

УДК 003.26:004.056.55

I. О. Розломий

Черкаський національний університет імені Богдана Хмельницького, Україна

**МАТЕМАТИЧНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТРОННИХ
ДОКУМЕНТІВ**

I.O. Rozlomi

**MATHEMATICAL MODEL OF INFORMATION SECURITY OF ELECTRONIC
DOCUMENTS**

Сучасний етап розвитку суспільства характеризується високим ступенем його інформатизації і зростаючою роллю комп'ютерних технологій. Обсяг інформації, збереженої в електронному вигляді, зріс у тисячі разів. Надійний електронний обмін даними можливий лише за умови забезпечення їх конфіденційності, надійного захисту від підробки чи несанкціонованого редагування та інших факторів пов'язаних з фальсифікацією і відмовою від авторства.

В електронному середовищі процес обробки документованої інформації представляє собою складний організаційно-технічний процес, що супроводжується загрозами інформаційної безпеки (ІБ). Інформаційній безпеці зараз приділяється багато уваги на всіх рівнях, починаючи від фізичних осіб і закінчуючи державою. Особливої актуальності завдання ІБ набуває в зв'язку з впровадженням технічних засобів обробки, передачі та зберігання інформації в усі сфери людської діяльності [1].

ІБ електронних документів (ЕД) – властивість системи електронного документообігу (СЕД) протидіяти несанкціонованому доступу до ЕД і неможливості їх модифікації. Порушення правил розмежування доступу може стати причиною порушення цілісності, достовірності та конфіденційності ЕД. Порушення ІБ – сукупність умов і факторів (явищ, дій, процесів), що спричиняють потенційну небезпеку, що призводить до непередбачуваних фактів таких, як витік інформації, модифікація та знищення інформації [2]. Визначення безпеки ЕД включає три основні складові: забезпечення цілісності, конфіденційності та доступності.

Цілісність ЕД – характеризує їх незмінність, достовірність, повноту інформації, що містять ЕД, тобто така їх властивість, яка гарантує чітко визначену структуру ЕД [3]. Порушення цілісності – це загрози, при реалізації яких інформація втрачає значимість, юридичну силу. Загрози цілісності інформації, що зберігається в СЕД чи передається по каналах зв'язку, які спрямовані на її редагування чи спотворення, що призводять до порушення якості чи повного знищення. Порушення цілісності інформації може мати випадковий і навмисний характер.

Відповідно [4], «конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов». Порушення конфіденційності може виникнути, як наслідок крадіжки, перехоплення інформації, зміни маршрутів руху ЕД. Загрози порушення конфіденційності спрямовані на розголошення конфіденційної чи секретної інформації. В разі реалізації цих загроз інформація стає відомою для суб'єктів, які не мають до неї доступу [5].

Доступність – це властивість ЕД, яка передбачає відсутність перешкод доступу до них і правомірному їх використанню власником чи уповноваженими суб'єктами. Доступність характеризує можливість несанкціонованого доступу до документів, що зберігаються в СЕД в будь-який момент часу. Класифікація порушень інформаційної безпеки ЕД показана на рисунку 1.

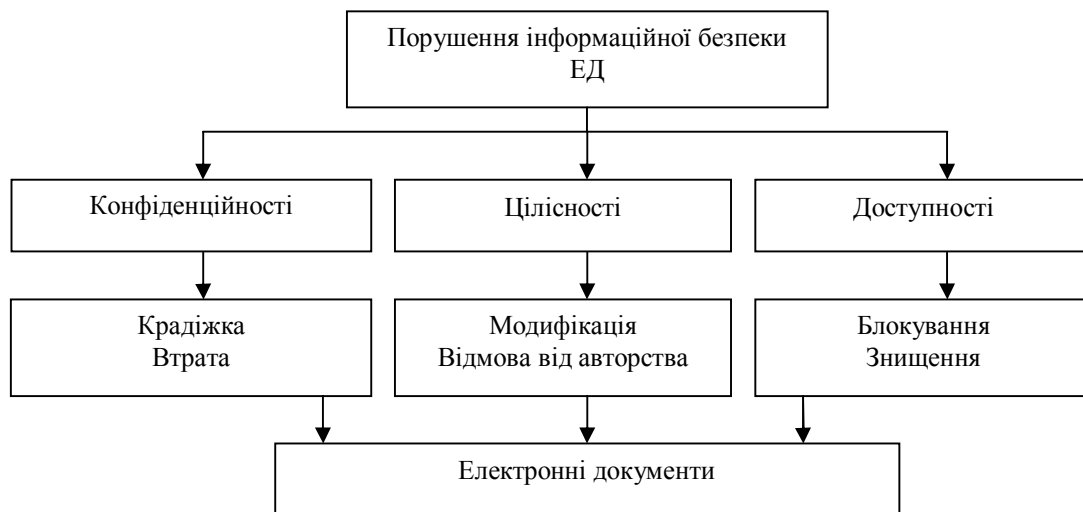


Рис. 1. Порушення інформаційної безпеки ЕД

Враховуючи основні властивості електронних документів, математичну модель інформаційної безпеки ЕД можна представити в вигляді задачі (1).

$$\sum_i^n f(C_i, K_i, D_i) \rightarrow \max \quad (1)$$

де $f(C_i, K_i, D_i)$ – значення функції ІБ для i -ї загрози безпеці, n – кількість загроз безпеці ЕД, C_i, K_i, D_i – ймовірності порушення цілісності, конфіденційності та достовірності ЕД для i -ї загрози.

Таким чином, захищена СЕД має передбачувати реалізацію, як мінімум таких механізмів захисту: забезпечення цілісності, безпечного доступу, конфіденційності та достовірності документів [6].

Обробка ЕД в СЕД сприяє якісному формуванню інформаційних ресурсів і забезпеченню їх ефективного функціонування. Використання СЕД дозволяє отримати гнучкість при обробці документів, значно підвищити ефективність роботи всієї структури, для якої вони призначені. Проте, використання СЕД призводить до необхідності розробки нових методів в області інформаційних технологій, які б забезпечували не лише оперативну обробку даних, а і їх безпеку. СЕД має забезпечувати надійний захист від можливих порушень безпеки, що вимагає великої кількості правових, організаційних та програмно-технічних заходів, що дозволять запобігти реалізації загроз ІБ.

Література

1. Королев И.Д. Анализ безопасности информации при применении модели отнесения документов автоматизированной системы к информационным областям ответственности исполнителей, Научный журнал КубГАУ. – 2013. – №93(09). – 11 с.
2. Певнев В.Я. Эффективность информационной безопасности замкнутых систем/ В.Я. Певнев// Радиоелектронні і комп'ютерні системи. – 2009. – № 5. – с. 82-85.
3. Домарев В.В. Безопасность информационных технологий. Системный подход/ В.В. Домарев – К.: ООО «ТИД «ДС». – 2004. – 992 с.
4. Закон України «Про інформацію»// Відомості Верховної Ради. – 1992. – № 48.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком. – 2000. – 452 с.
6. Ярочкин В.И. Информационная безопасность// В.И. Ярочкин. – М.: Фонд «Мир»: Акад. Проект. – 2003. – 640 с.